SWS Computersysteme AG

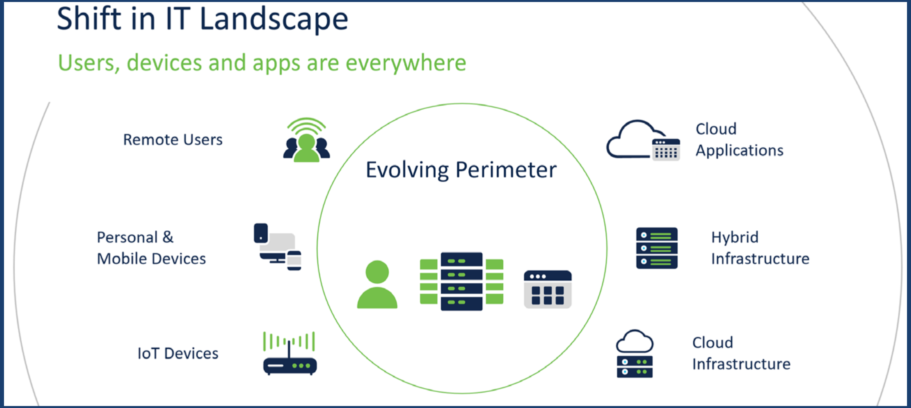
SWS COMPUTERSYSTEME
Member of ACP Group

Cisco Identity Services Engine (ISE)
Cisco Secure Access by DUO –
Segmentierung und Zero Trust

Agenda

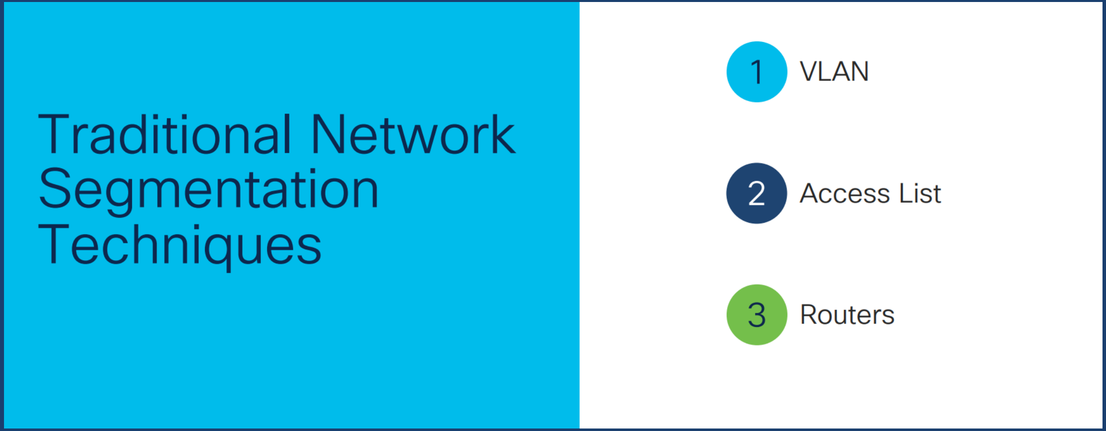
- Zero Trust und Netzwerksegmentierung
- Cisco Identity Services Engine (ISE)
- Cisco Identity Services Engine (ISE) - Demo
- Cisco Secure Access by DUO
- Cisco Secure Access by DUO - Demo
- Q&A

Zero Trust und Netzwerksegmentierung



Shift in IT Landscape

Users, devices and apps are everywhere



Traditional Network Segmentation Techniques

1 VLAN

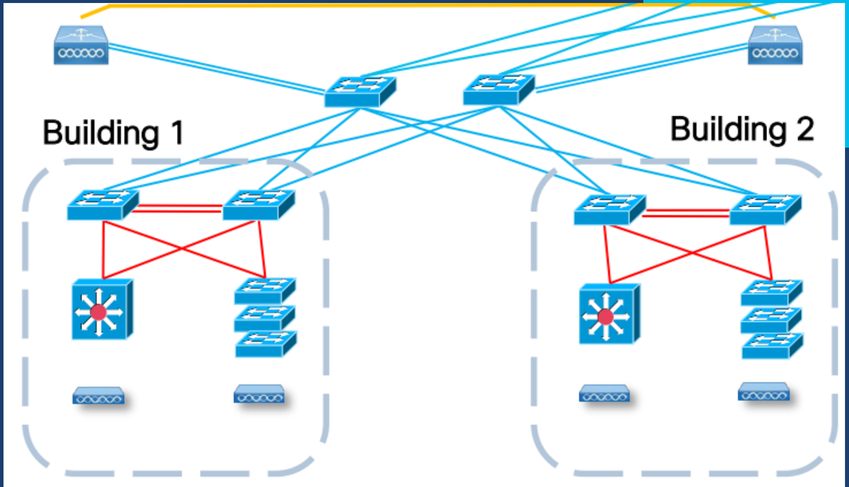
2 Access List

3 Routers

Zero Trust und Netzwerksegmentierung

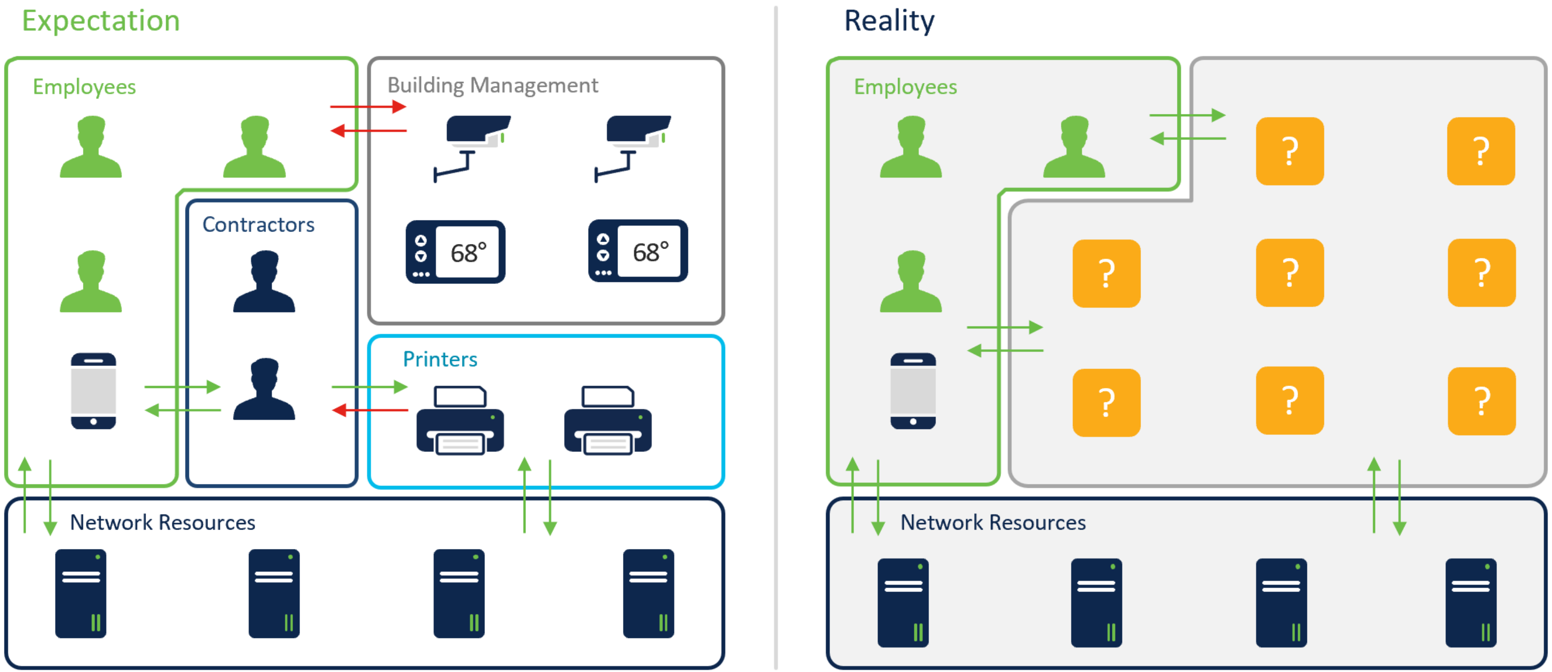
The Challenges

1. Not scalable
2. Tedious to manage
3. Large access lists



Zero Trust und Netzwerksegmentierung

Least Privilege Access: Expectation vs. Reality



Zero Trust und Netzwerksegmentierung

Cisco Secure Zero Trust

A comprehensive approach to securing all access across your networks, applications, and environment.

Workforce

Ensure only the right users and secure devices can access applications.

Workloads

Secure all connections within your apps, across multi-cloud.

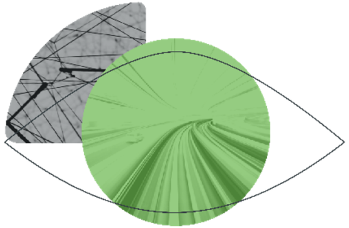
Workplace

Secure all user and device connections across your network, including IoT.

Zero Trust und Netzwerksegmentierung

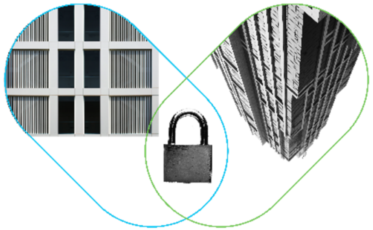
The Foundations of Zero Trust in Your Workplace

Visibility



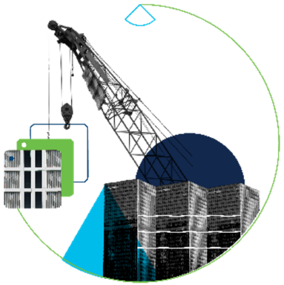
Grant the right level of network access to users across domains

Segmentation



Shrink zones of trust and grant access based on least privilege

Containment



Automate containment of infected endpoints and revoke network access

SWS COMPUTERSYSTEME
Member of ACP Group

Zero Trust für Workforce und Workplace

- Cisco Identity Services Engine
- Cisco Secure Access by DUO

Quelle: www.cisco.de

Agenda

- Zero Trust und Netzwerksegmentierung
- Cisco Identity Services Engine (ISE)
- Cisco Identity Services Engine (ISE) - Demo
- Cisco Secure Access by DUO
- Cisco Secure Access by DUO - Demo
- Q&A

Cisco Identity Services Engine

ISE Provides Zero Trust for the Workplace

Enterprise

Security

Endpoints

- Users
- Devices
- Things

Network Devices

- Switches
- WLCs / APs
- VPN

Cisco ISE

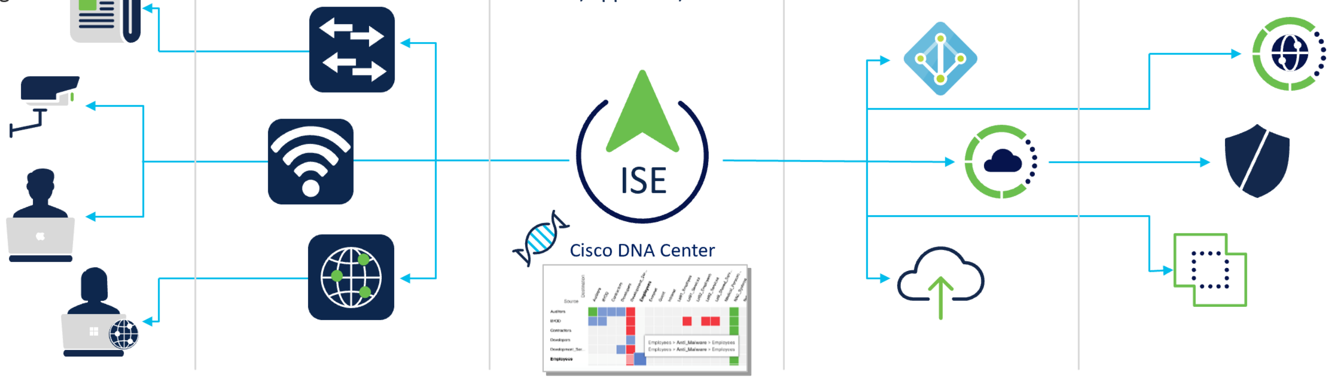
- Standalone ISE
- Multi-node ISE
- VM/Appliance/Cloud

Identity Services

- Azure/AD/LDAP
- MDM
- SAML/MFA

Security Services

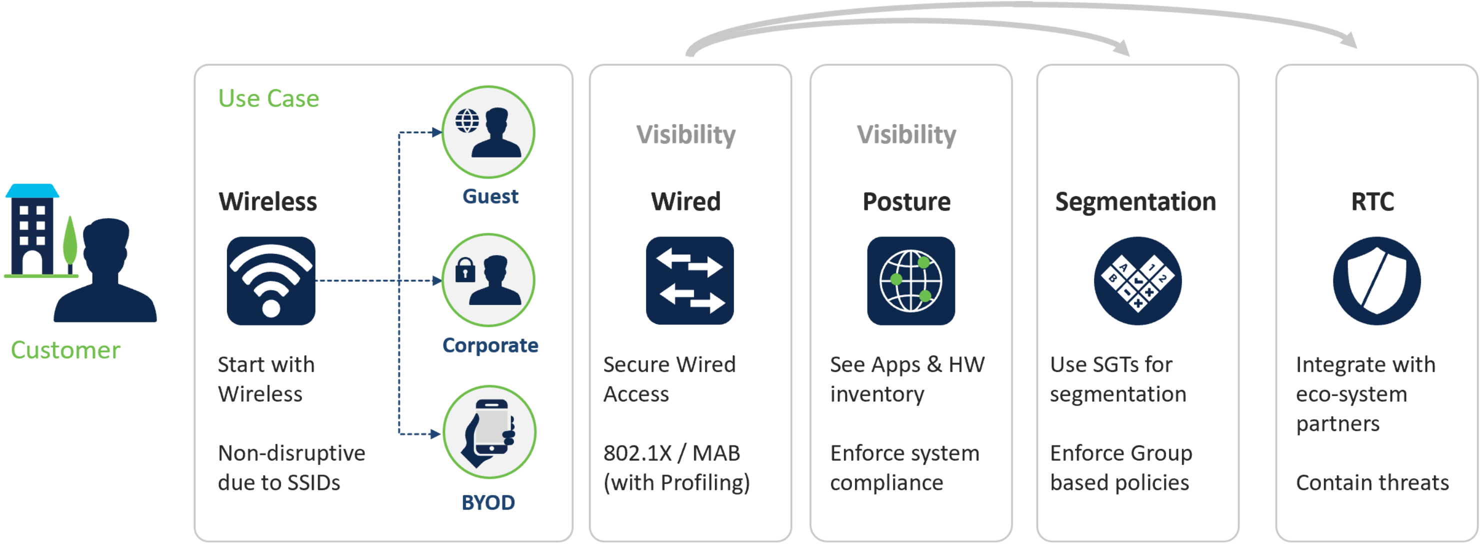
- Cloud Analytics
- Secure Firewall
- Partners



Cisco Identity Services Engine

A Typical Customer Journey

Not a standard or recommended approach
Each use case may be the end goal



Customer

Use Case

Wireless

Start with Wireless

Non-disruptive due to SSIDs

Guest

Corporate

BYOD

Visibility

Wired

Secure Wired Access

802.1X / MAB (with Profiling)

Visibility

Posture

See Apps & HW inventory

Enforce system compliance

Segmentation

Use SGTs for segmentation

Enforce Group based policies

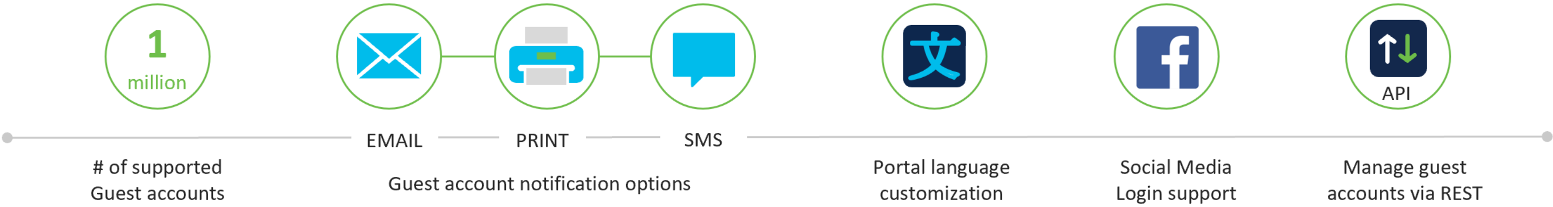
RTC

Integrate with eco-system partners

Contain threats

Cisco Identity Services Engine

Guest Solution Overview



EMAIL — PRINT — SMS

# of supported
Guest accounts

Guest account notification options

Portal language
customization

Social Media
Login support

Manage guest
accounts via REST

The 3 types of guest access

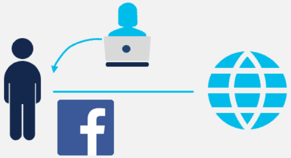
Hotspot

Immediate, un-credentialed
Internet access

Self Registered

Self-registration by guests, Sponsors may
approve access

Sponsored Guest Access

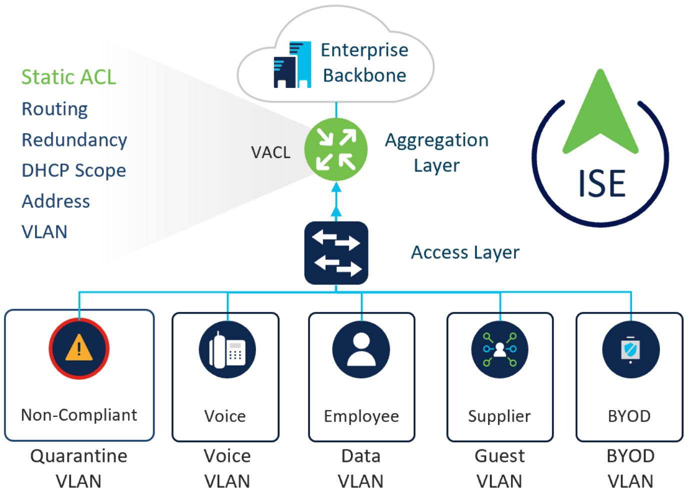


Authorized sponsors create account and
share credentials

Cisco Identity Services Engine

Group Based Policy Simplifies Segmentation

Traditional Segmentation

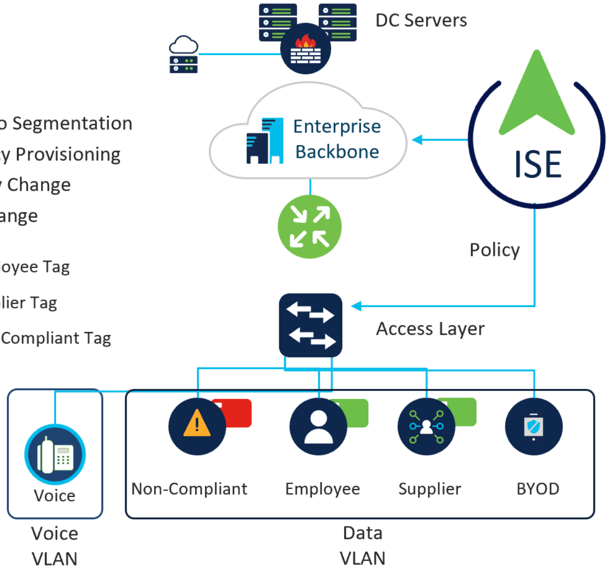


Security Policy based on Topology
High cost and complex maintenance

TrustSec

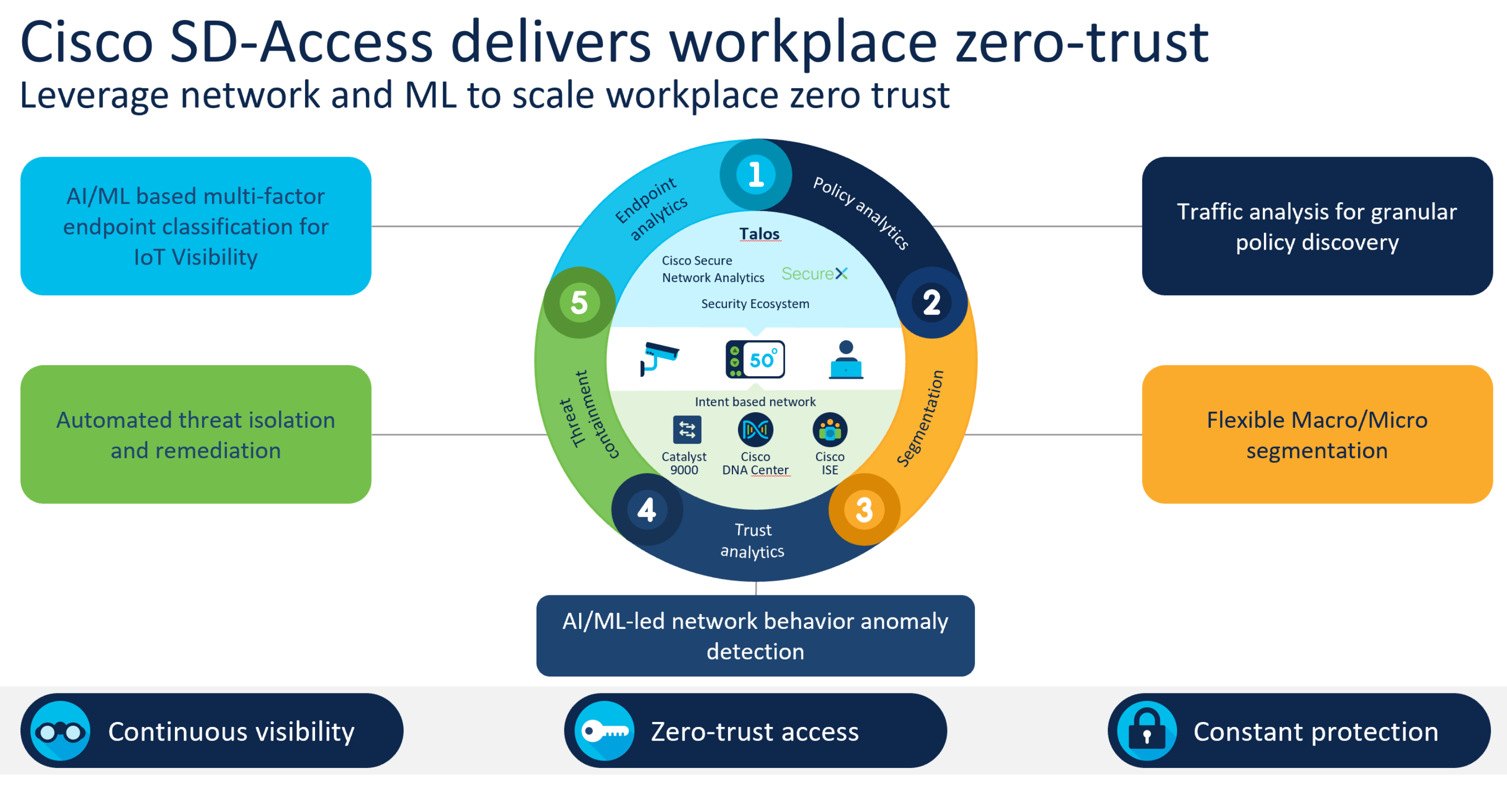
Micro/Macro Segmentation
Central Policy Provisioning
No Topology Change
No VLAN Change

🟩 Employee Tag
🟨 Supplier Tag
🟥 Non-Compliant Tag



Use existing topology and automate security policy to reduce OpEx

Cisco Identity Services Engine



Cisco SD-Access delivers workplace zero-trust

Leverage network and ML to scale workplace zero trust

AI/ML based multi-factor endpoint classification for IoT Visibility

Automated threat isolation and remediation

Traffic analysis for granular policy discovery

Flexible Macro/Micro segmentation

AI/ML-led network behavior anomaly detection

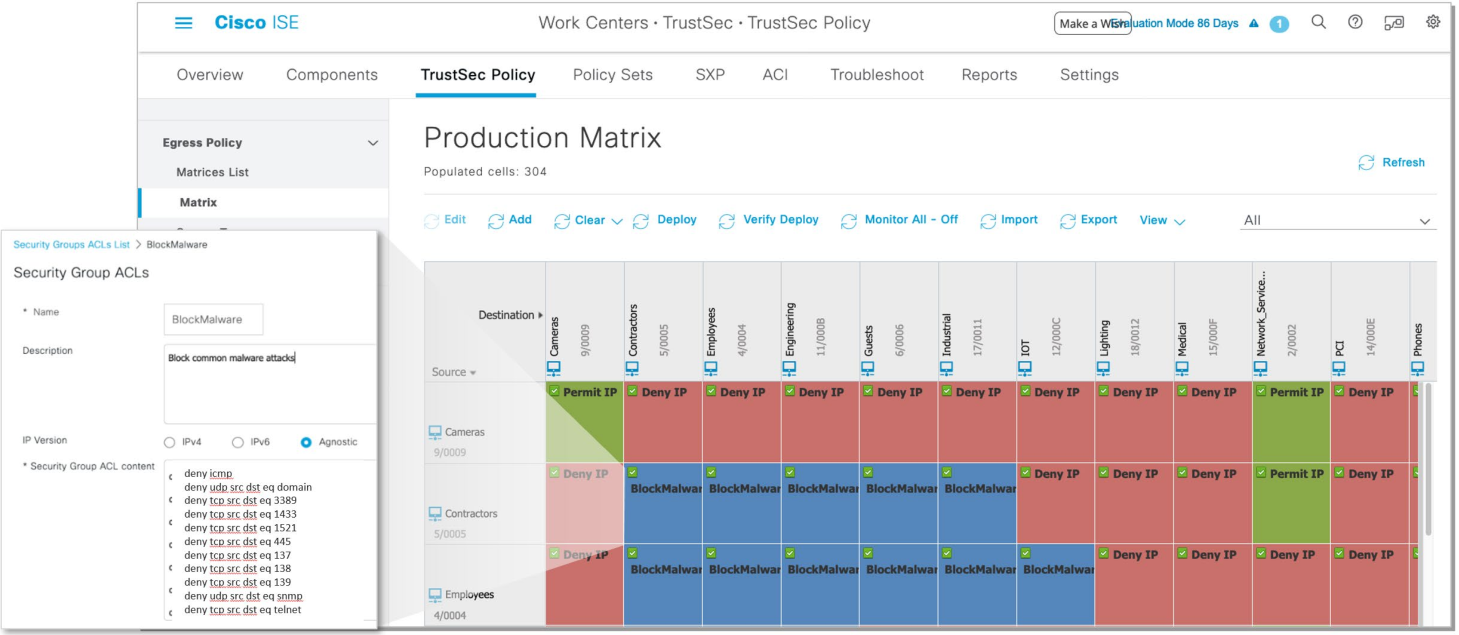
Continuous visibility

Zero-trust access

Constant protection

Cisco Identity Services Engine

Non-Fabric Group-Based Policy Enforcement



Security Groups ACLs List > BlockMalware

Security Group ACLs

* Name: BlockMalware

Description: Block common malware attacks

IP Version: ○ IPv4 ○ IPv6 ● Agnostic

* Security Group ACL content

```
deny icmp
deny udp src dst eq domain
deny tcp src dst eq 3389
deny tcp src dst eq 1433
deny tcp src dst eq 1521
deny tcp src dst eq 445
deny tcp src dst eq 137
deny tcp src dst eq 138
deny tcp src dst eq 139
deny udp src dst eq snmp
deny tcp src dst eq telnet
```

Production Matrix

Populated cells: 304

Source ▾ / Destination ▸	Cameras 9/0009	Contractors 5/0005	Employees 4/0004	Engineering 11/000B	Guests 6/0006	Industrial 17/0011	IOT 12/000C	Lighting 18/0012	Medical 15/000F	Network_Service... 2/0002	PCI 14/000E	Phones
Cameras 9/0009	☑ Permit IP	☑ Deny IP	☑ Deny IP	☑ Deny IP	☑ Deny IP	☑ Deny IP	☑ Deny IP	☑ Deny IP	☑ Deny IP	☑ Permit IP	☑ Deny IP	☑
Contractors 5/0005	☑ Deny IP	☑ BlockMalwar	☑ BlockMalwar	☑ BlockMalwar	☑ BlockMalwar	☑ BlockMalwar	☑ Deny IP	☑ Deny IP	☑ Deny IP	☑ Permit IP	☑ Deny IP	☑
Employees 4/0004	☑ Deny IP	☑ BlockMalwar	☑ BlockMalwar	☑ BlockMalwar	☑ BlockMalwar	☑ BlockMalwar	☑ BlockMalwar	☑ Deny IP	☑ Deny IP	☑ Deny IP	☑ Deny IP	☑

Cisco Identity Services Engine

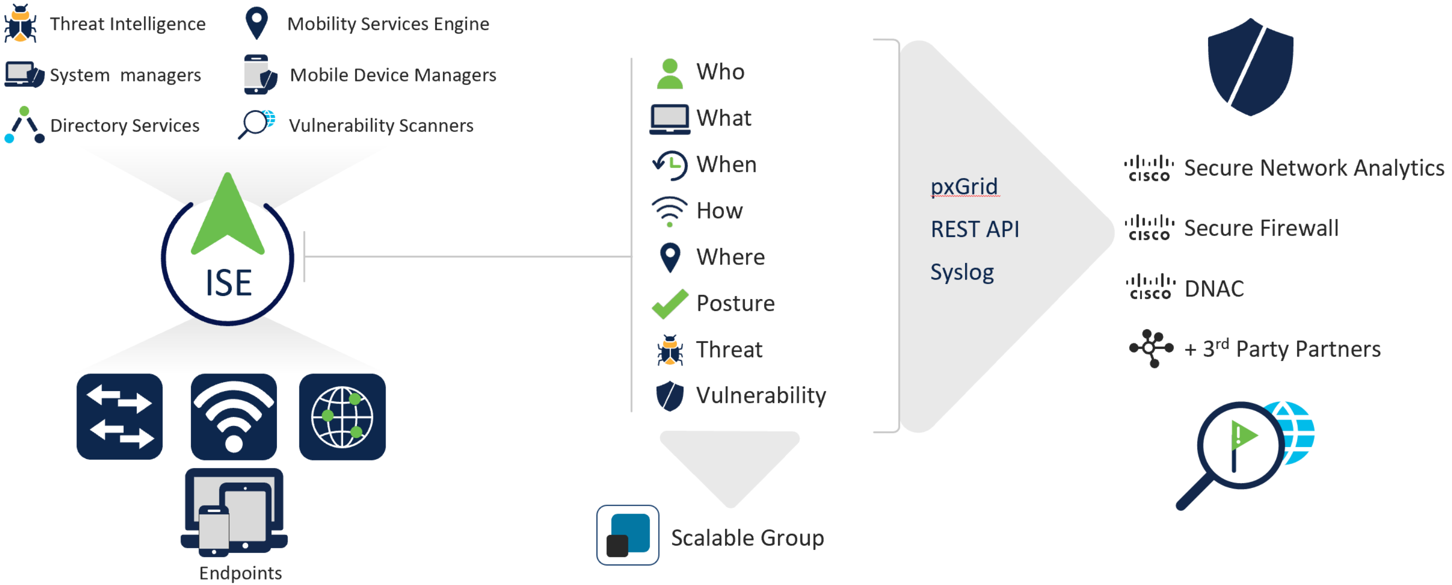
Context Build, Summarize, Exchange

Visibility and Access Control

ISE builds context and applies access control restrictions to users and devices

Context Reuse

by eco-system partners for analysis & control



- Threat Intelligence
- Mobility Services Engine
- System managers
- Mobile Device Managers
- Directory Services
- Vulnerability Scanners

ISE

Endpoints

- Who
- What
- When
- How
- Where
- Posture
- Threat
- Vulnerability

Scalable Group

pxGrid

REST API

Syslog

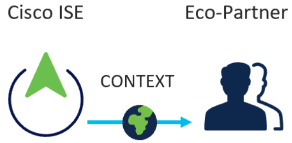
- Secure Network Analytics
- Secure Firewall
- DNAC
- + 3rd Party Partners

Cisco Identity Services Engine

Context Sharing with pxGrid

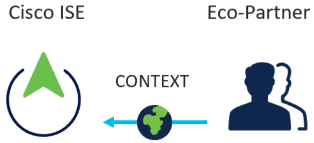
Eco system partnership to enrich, exchange context and enact

Context to Partner



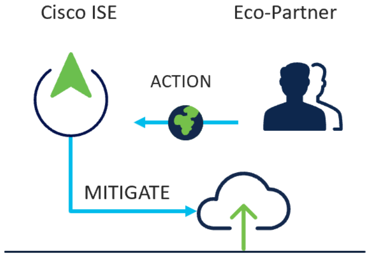
ISE makes Customer
IT Platforms User/Identity,
Device and Network Aware

Enrich ISE Context



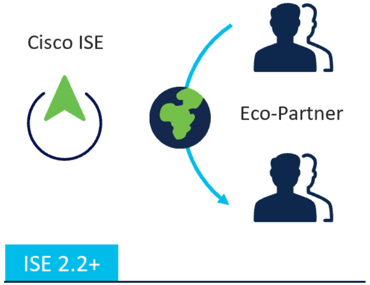
Enrich ISE context. Make ISE a better Policy Enforcement Platform

Threat Mitigation



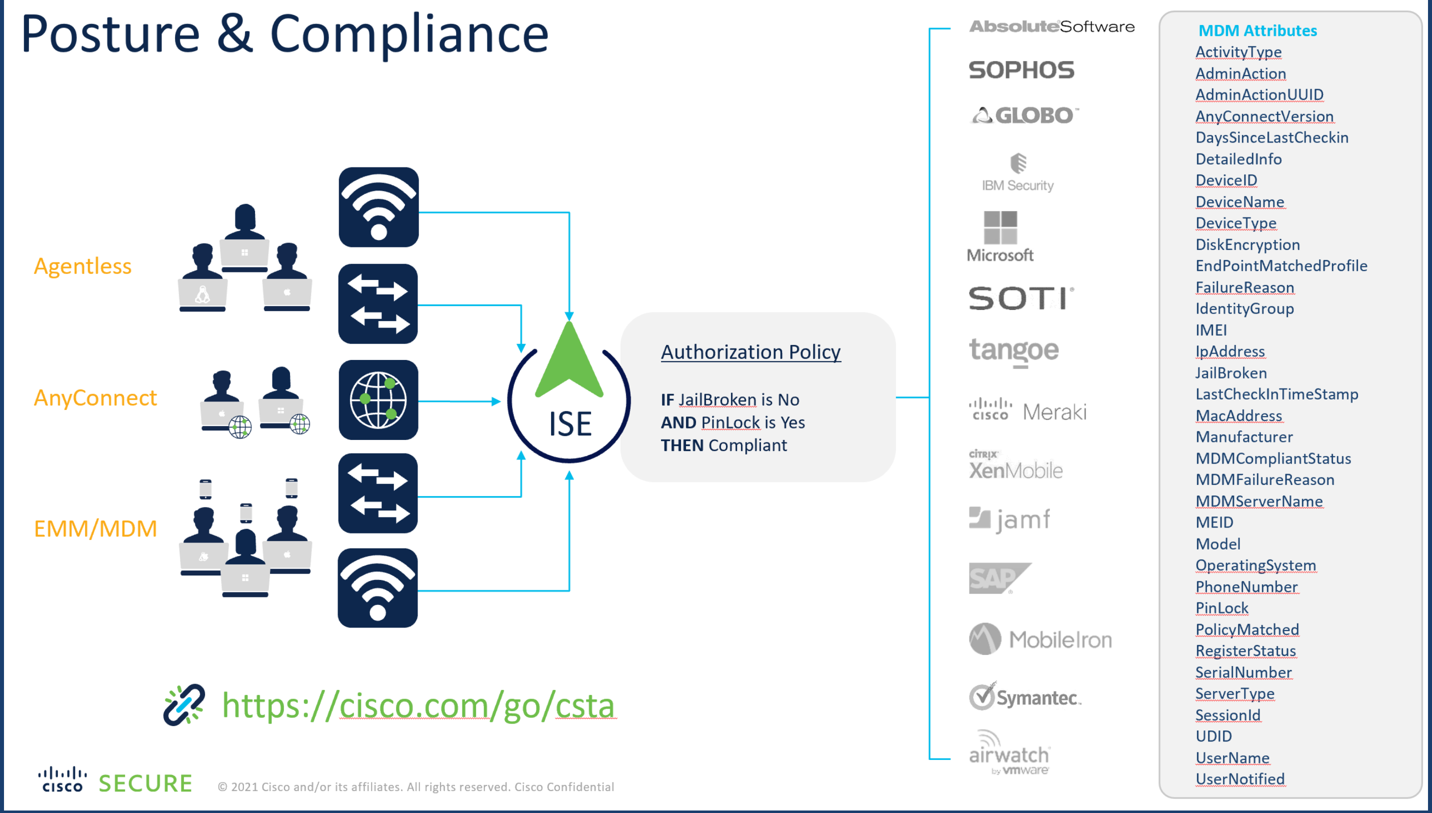
Enforce dynamic policies into the network based on Partner's request

Context Brokerage



ISE brokers Customer's IT platforms to share data amongst themselves

Cisco Identity Services Engine



Posture & Compliance

Authorization Policy

IF JailBroken is No
AND PinLock is Yes
THEN Compliant

MDM Attributes

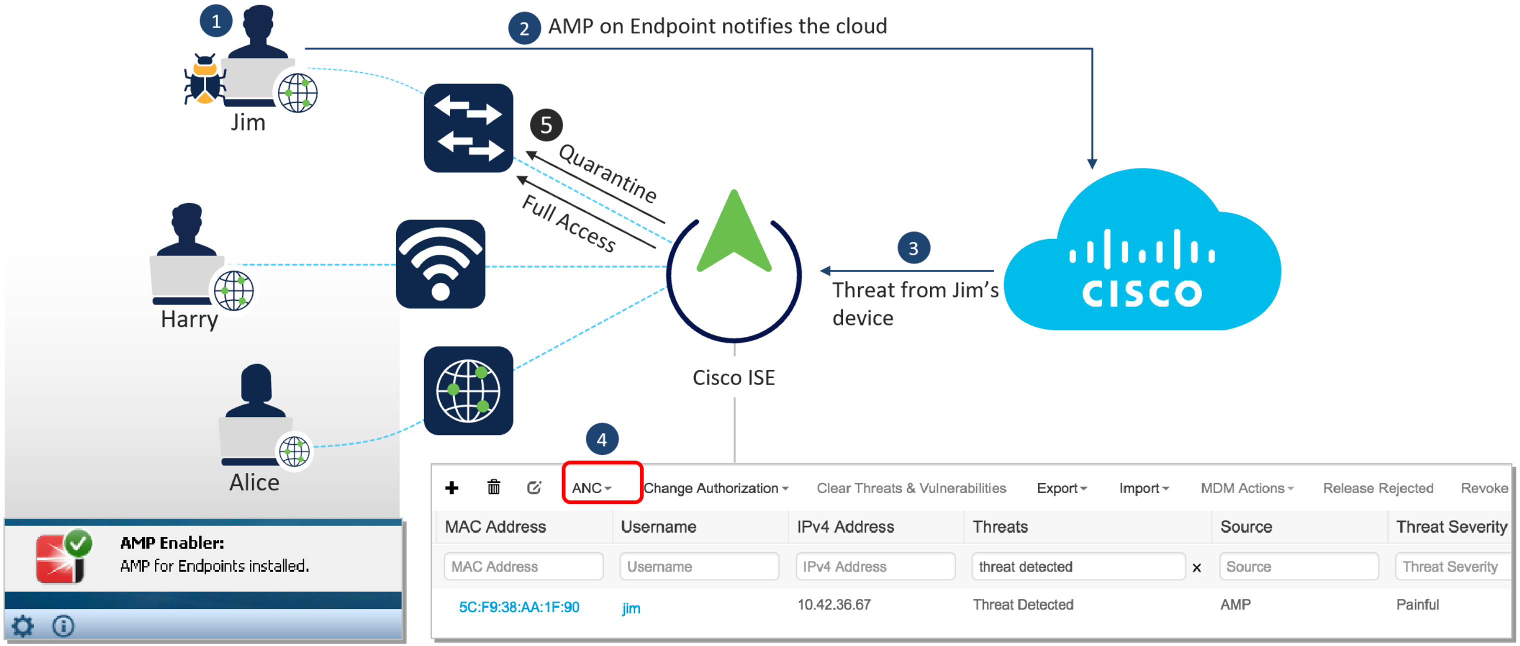
- ActivityType
- AdminAction
- AdminActionUUID
- AnyConnectVersion
- DaysSinceLastCheckin
- DetailedInfo
- DeviceID
- DeviceName
- DeviceType
- DiskEncryption
- EndPointMatchedProfile
- FailureReason
- IdentityGroup
- IMEI
- IpAddress
- JailBroken
- LastCheckInTimeStamp
- MacAddress
- Manufacturer
- MDMCompliantStatus
- MDMFailureReason
- MDMServerName
- MEID
- Model
- OperatingSystem
- PhoneNumber
- PinLock
- PolicyMatched
- RegisterStatus
- SerialNumber
- ServerType
- SessionId
- UDID
- UserName
- UserNotified

https://cisco.com/go/csta

cisco SECURE

Cisco Identity Services Engine

Threat Visibility Rapid Threat Containment (RTC)

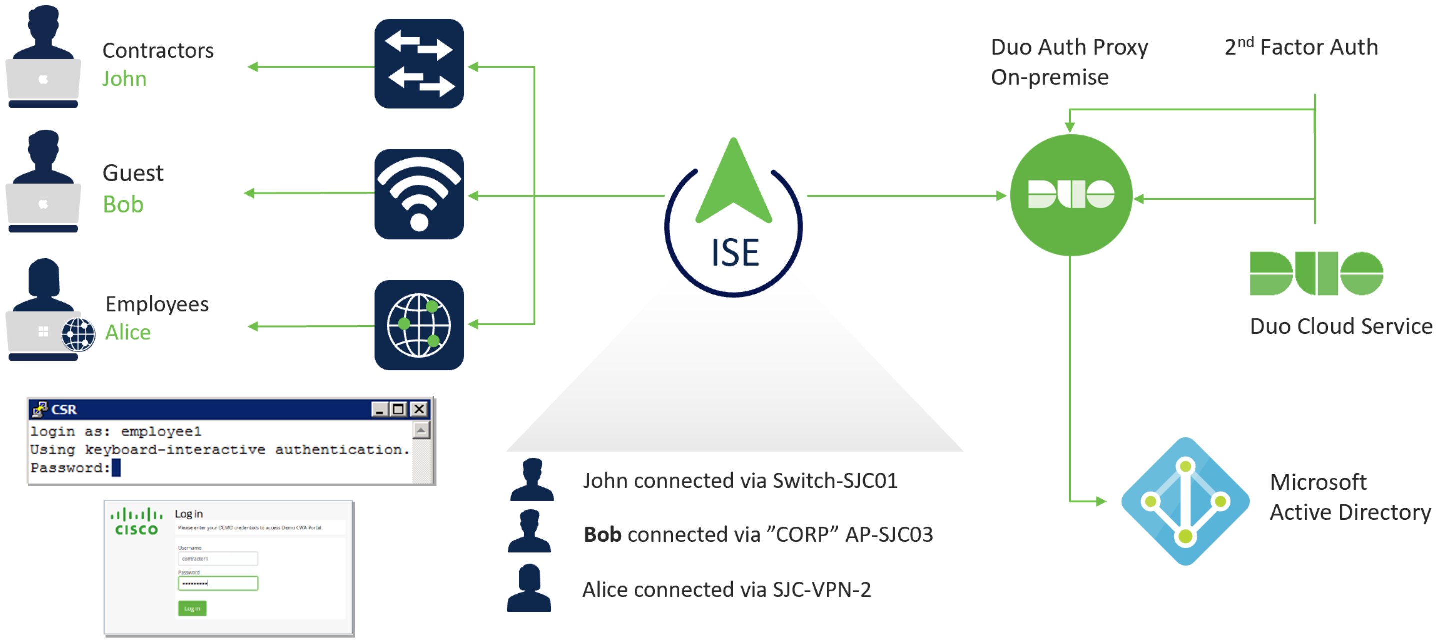


AMP Enabler:
AMP for Endpoints installed.

MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity
MAC Address	Username	IPv4 Address	threat detected ×	Source	Threat Severity
5C:F9:38:AA:1F:90	jim	10.42.36.67	Threat Detected	AMP	Painful

Cisco Identity Services Engine

ISE and Duo Integration for MFA



John connected via Switch-SJC01

Bob connected via ”CORP” AP-SJC03

Alice connected via SJC-VPN-2

```
CSR
login as: employee1
Using keyboard-interactive authentication.
Password:
```

Log in

Please enter your DEMO credentials to access Demo CWA Portal.

Username: contractor1

Password: •••••••••

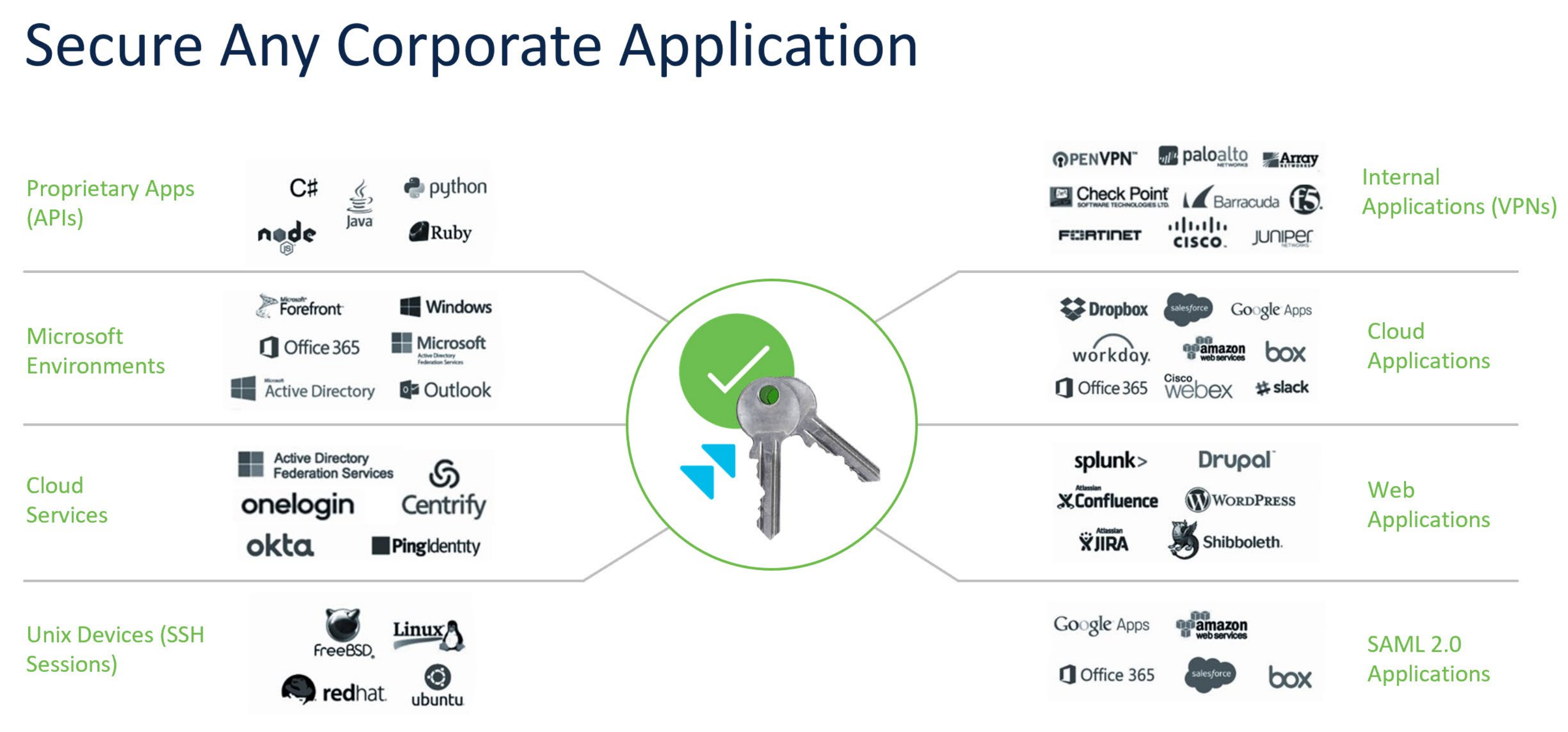
Agenda

- Zero Trust und Netzwerksegmentierung
- Cisco Identity Services Engine (ISE)
- Cisco Identity Services Engine (ISE) - Demo
- Cisco Secure Access by DUO
- Cisco Secure Access by DUO - Demo
- Q&A

Agenda

- Zero Trust und Netzwerksegmentierung
- Cisco Identity Services Engine (ISE)
- Cisco Identity Services Engine (ISE) - Demo
- Cisco Secure Access by DUO
- Cisco Secure Access by DUO - Demo
- Q&A

Cisco Secure Access by DUO



Secure Any Corporate Application

Proprietary Apps (APIs)

Microsoft Environments

Cloud Services

Unix Devices (SSH Sessions)

Internal Applications (VPNs)

Cloud Applications

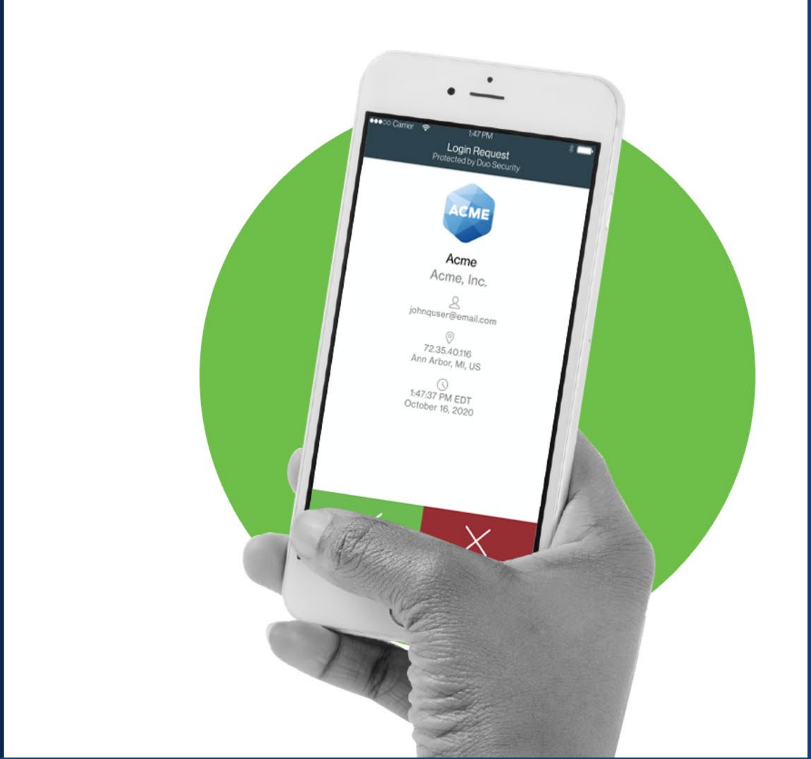
Web Applications

SAML 2.0 Applications

Cisco Secure Access by DUO

World’s Easiest and Most Secure MFA

- Instantly integrates with all apps
- Users self-enroll in minutes
- Users authenticate in seconds; no codes to enter



Cisco Secure Access by DUO

Broadest Range of Multi-Factor Authentication (MFA) Options

- Configure authentication options for each application or group of users
- Enable multiple option for users for ease of use and flexibility

- Wearables
- Push
- Phone Call
- Soft Token
- Biometrics
- U2F
- Hardware Tokens
- SMS

Cisco Secure Access by DUO

Duo Supports Your Work Applications

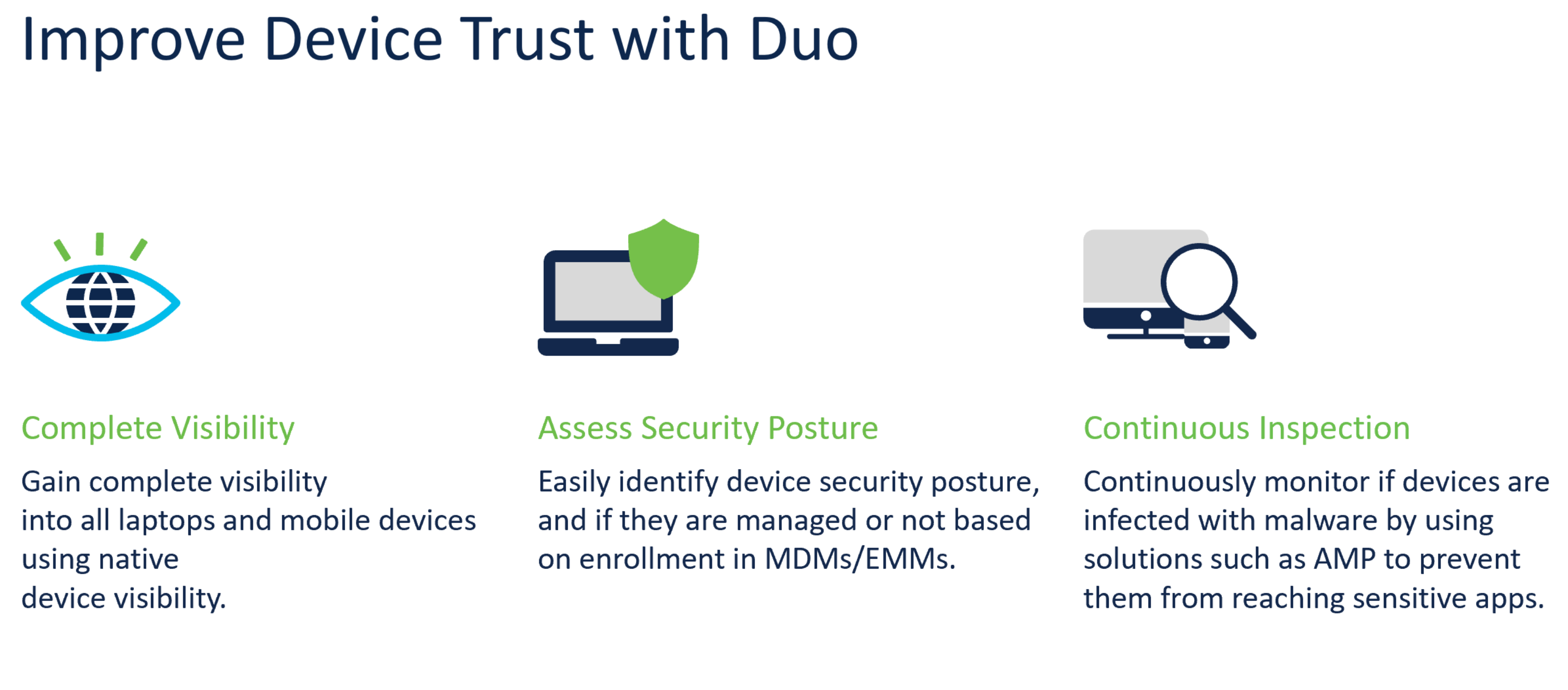
Start Here			Then Expand		
VPN RA	Multicloud	Email/MSFT	On-Prem	SSO	Custom
cisco	Google Apps	Office 365	Epic	Microsoft Azure	REST APIS
JUNIPER NETWORKS	salesforce	Outlook	ORACLE PEOPLESOFT	AD FS	WEB SDK
CITRIX	aws	Microsoft Remote Desktop Services	vmware Horizon View	okta	RADIUS
paloalto NETWORKS	box	Windows Server	>_SSH	Centrify	SAML
Pulse Secure	Dropbox	RRAS	Shibboleth	onelogin	OIDC

Cisco Secure Access by DUO

Device Trust

Assess the health and security posture of any device

Cisco Secure Access by DUO



Improve Device Trust with Duo

Complete Visibility

Gain complete visibility into all laptops and mobile devices using native device visibility.

Assess Security Posture

Easily identify device security posture, and if they are managed or not based on enrollment in MDMs/EMMs.

Continuous Inspection

Continuously monitor if devices are infected with malware by using solutions such as AMP to prevent them from reaching sensitive apps.

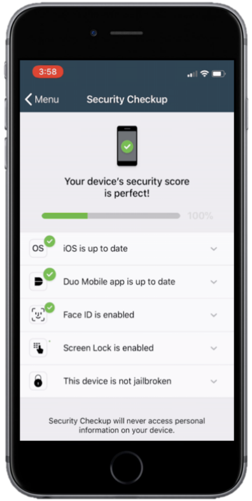
Cisco Secure Access by DUO

Assess Security Posture

Easily identify device security posture.

- Is it managed?
- Is it running up to date software?
- Is it encrypted?
- Is it passcode protected?
- Is the firewall enabled?
- Is biometric enabled?

Duo Mobile App



3:58

Menu

Security Checkup

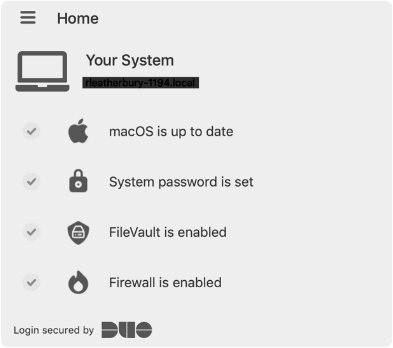
Your device's security score is perfect!

100%

- iOS is up to date
- Duo Mobile app is up to date
- Face ID is enabled
- Screen Lock is enabled
- This device is not jailbroken

Security Checkup will never access personal information on your device.

Duo Device Health App



Home

Your System

[redacted]

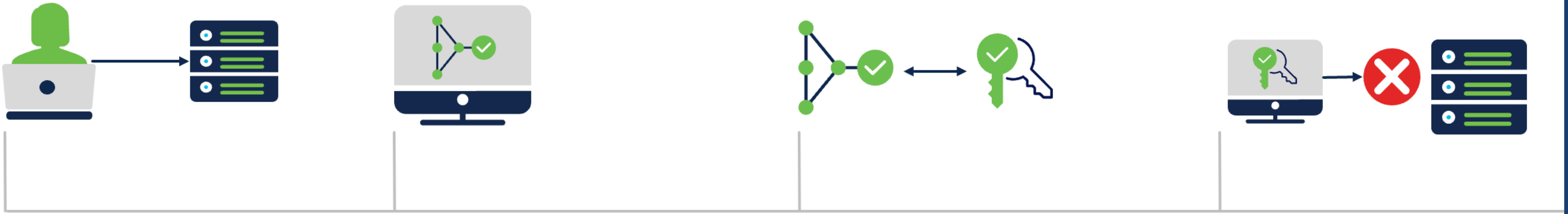
- ✓ macOS is up to date
- ✓ System password is set
- ✓ FileVault is enabled
- ✓ Firewall is enabled

Login secured by DUO

Cisco Secure Access by DUO

Continuous Inspection

Duo and Secure Endpoint work together to provide stronger access security



Users use their devices to access application

Cisco Secure Endpoint running on the device detected malware

Cisco Secure Endpoint notifies Duo about the infected device

Duo blocks that device from accessing apps

Cisco Secure Access by DUO

Feature Highlights

Duo MFA

- Multi-Factor Authentication
- Single Sign-On (SSO)
- Protect Any Application
- Protect Federated Cloud Apps

Duo Access

- Duo MFA +
- Adaptive Groups Based Policy Controls
- User Based Policy
- Device Visibility
- Device Health Checks
- Device Based Policy

Duo Beyond

- Duo MFA and Access +
- 3rd Party Agent Verification
- Trusted Endpoints
- Secure Remote Access
- Duo Mobile as Trusted

Agenda

- Zero Trust und Netzwerksegmentierung
- Cisco Identity Services Engine (ISE)
- Cisco Identity Services Engine (ISE) - Demo
- Cisco Secure Access by DUO
- Cisco Secure Access by DUO - Demo
- Q&A

Vielen Dank für Ihre Aufmerksamkeit.

Fragen?